

1 / 20

FIG. 1

ITEM	DESCRIPTION
Version 1	
version	VERSION OF FORMAT OF CERTIFICATE
serial Number	SERIAL NUMBER OF CERTIFICATE, SPECIFIED BY CERTIFICATION AUTHORITY
signature algorithm Identifier algorithm parameters	SIGNATURE ALGORITHM AND ITS PARAMETERS OF CERTIFICATE
issuer	NAME OF CERTIFICATION AUTHORITY (IN DISTINGUISHED NAME FORMAT)
validity not Before not After	EFFECTIVE PERIOD OF CERTIFICATE START DATE END DATE
subject	NAME FOR IDENTIFYING USER
subject Public Key Info algorithm subject Public key	PUBLIC-KEY INFORMATION OF USER KEY ALGORITHM KEY INFORMATION
Version 3	
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	FOR IDENTIFYING KEY USED FOR VERIFYING SIGNATURE OF CERTIFICATION AUTHORITY KEY IDENTIFICATION NUMBER (IN OCTAL) NAME OF CERTIFICATION AUTHORITY (IN GENERAL NAME FORMAT) AUTHENTICATION NUMBER
subject key Identifier	IDENTIFIER OF EACH KEY, USED WHEN PLURALITY OF KEYS ARE CERTIFIED
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key Cert Sign (6)CRL Sign (7)encipher Only (8)decipher Only	FOR SPECIFYING USE OBJECTIVE OF KEY (0) FOR DIGITAL SIGNATURE (1) FOR REPUDIATION PREVENTION (2) FOR ENCRYPTING KEY (3) FOR ENCRYPTING MESSAGE (4) FOR DISTRIBUTING COMMON KEY (5) FOR VERIFYING SIGNATURE IN AUTHENTICATION (6) FOR VERIFYING SIGNATURE IN INVALIDITY LIST (7) ONLY FOR ENCRYPTING DATA WHEN KEY IS CHANGED (8) ONLY FOR DECRYPTING DATA WHEN KEY IS CHANGED
private Key Usage Period not Before not After	EFFECTIVE PERIOD OF PRIVATE KEY HELD BY USER

FIG. 2

Certificate Policy policy Identifier policy Qualifiers	CERTIFICATE ISSUING POLICY OF CERTIFICATION AUTHORITY POLICY ID AUTHENTICATION STANDARD
policy Mappings issuer Domain Policy subject Domain Policy	REQUIRED ONLY FOR AUTHENTICATING CERTIFICATION AUTHORITY. SPECIFIES MAPPING BETWEEN POLICY OF CERTIFICATION AUTHORITY AND POLICY OF OBJECT TO BE AUTHENTICATED
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	DEFINES ATTRIBUTE OF DIRECTORY (X.500). USED FOR REPORTING ATTRIBUTE IN ADVANCE WHEN COMMUNICATION MATE USES DIRECTORY INFORMATION
subject Alt Name	ALIAS OF USER (IN GENERAL NAME FORMAT)
issuer Alt Name	ALIAS OF CERTIFICATE ISSUER
subject Directory Attributes	ANY ATTRIBUTE OF USER
basic Constraints CA path Len Constraint	DETERMINES WHETHER PUBLIC KEY TO BE CERTIFIED IS FOR SIGNATURE OF CERTIFICATION AUTHORITY OR USER'S
name Constraints permitted Subtrees base minimum maximum excluded Subtrees	USED ONLY WHEN PARTY TO BE AUTHENTICATED IS CERTIFICATION AUTHORITY (CA AUTHENTICATION)
policy Constraints require Explicit Policy inhibit Policy Mapping	DESCRIBES CONSTRAINT WHICH REQUESTS A CLEAR AUTHENTICATION POLICY ID FOR REMAINING AUTHENTICATION PATH OR PROHIBITION POLICY MAP
CRL Distribution Points	DESCRIBES REFERENCE POINT IN INVALIDATION LIST USED, WHEN USER USES CERTIFICATE, FOR CHECKING IF CERTIFICATE HAS NOT LAPSED
SIGNATURE	SIGNATURE OF ISSUER

FIG. 3

ITEM		DESCRIPTION		
acinfo	AttributeCertificateInfo			
	version	AttCertVersion		VERSION OF FORMAT OF ATTRIBUTE CERTIFICATE
	holder	Holder		IDENTIFIES OWNER OF PUBLIC-KEY CERTIFICATE WITH WHICH ATTRIBUTE CERTIFICATE IS ASSOCIATED
		baseCertificateId	issuerSerial	
			issuer	NAME OF ISSUER OF PUBLIC-KEY CERTIFICATE OF OWNER OF ATTRIBUTE CERTIFICATE
			serial	SERIAL NUMBER OF ISSUER OF PUBLIC-KEY CERTIFICATE OF OWNER OF ATTRIBUTE CERTIFICATE
			issuerUID	UNIQUE IDENTIFIER OF ISSUER OF PUBLIC-KEY CERTIFICATE OF OWNER OF ATTRIBUTE CERTIFICATE
		entityName		NAME OF OWNER OF ATTRIBUTE CERTIFICATE
		objectDigestInfo	objectDigestInfo	ASSUMING THAT ATTRIBUTE CERTIFICATE IS NOT LINKED TO IDENTIFICATION INFORMATION OR PUBLIC-KEY CERTIFICATE IN FUTURE
			digestedObjectType	
			otherObjectTypeID	
			digestAlgorithm	
			objectDigest	
	issuer	AttCertIssuer		SPECIFIES NAME OF ISSUER WHO SIGNED ATTRIBUTE CERTIFICATE
		v2Form	V2Form	
			issuerName	NAME OF ISSUER OF ATTRIBUTE CERTIFICATE
			baseCertificateId	
			objectDigestInfo	
	signature	AlgorithmIdentifier		IDENTIFIER OF ALGORITHM USED FOR MAKING SIGNATURE OF ATTRIBUTE CERTIFICATE EFFECTIVE
	serialNumber	CertificateSerialNumber		SERIAL NUMBER ASSIGNED BY ATTRIBUTE AUTHORITY TO EACH CERTIFICATE
	attCertValidityPeriod	AttCertValidityPeriod		EFFECTIVE PERIOD OF ATTRIBUTE CERTIFICATE
		notBefore		START DATE
		notAfter		END DATE

FIG. 4

attributes	Attribute	Attribute Type			INFORMATION RELATED TO PRIVILEGE OF OWNER OF ATTRIBUTE CERTIFICATE
	type				
		Service Authentication			DESCRIBES AUTHENTICATION INFORMATION RELATED TO SERVICE. USED WHEN VERIFIER OF ATTRIBUTE CERTIFICATE AUTHENTICATES OWNER
		service			
		ident			
		authInfo			
		Access Identity			ACCESS PERMISSION INFORMATION OF OWNER, USED BY VERIFIER OF ATTRIBUTE CERTIFICATE
		Charging Identity			INFORMATION FOR IDENTIFYING OWNER OF ATTRIBUTE CERTIFICATE FOR ACCOUNTING
		Group			BELONGING RELATION OF OWNER OF ATTRIBUTE CERTIFICATE, TO GROUP
		Role			ROLE ASSIGNED TO OWNER OF ATTRIBUTE CERTIFICATE
				roleAuthority	
				roleName	
		Clearance			INFORMATION RELATED TO USE PERMISSION OF CONFIDENTIAL INFORMATION, FOR OWNER OF ATTRIBUTE CERTIFICATE
				policyId	
				classList	
				securityCategories	
	values				
issuerUniqueId	uniqueIdentifier				USED WHEN SPECIFIED BY PUBLIC-KEY CERTIFICATE OF ISSUER OF ATTRIBUTE CERTIFICATE
extensinos					DESCRIBES NOT INFORMATION OF OWNER OF ATTRIBUTE CERTIFICATE BUT INFORMATION OF ATTRIBUTE CERTIFICATE
		Audit Identity			USED BY SERVER/SERVICE ADMINISTRATOR TO INSPECT OWNER OF ATTRIBUTE CERTIFICATE TO DETECT (SPECIFY) FRAUDULENT ACTIONS
		AC Targeting			DESCRIBES SERVER/SERVICE FOR WHICH ATTRIBUTE CERTIFICATE IS ISSUED
		Authority Key Identifier			KEY INFORMATION OF ISSUER OF ATTRIBUTE CERTIFICATE
		Authority Information Access			URI OF OCSP RESPONDER
		CRL Distribution Points			URI OF CRL DISTRIBUTION POINT
		No Revocation Available			INDICATES THAT THERE IS NO INVALIDITY INFORMATION CORRESPONDING TO ATTRIBUTE CERTIFICATE
		Proxy Info			ENTITY TO WHICH ATTRIBUTE CERTIFICATE CAN BE SUBMITTED
signature Algorithm	AlgorithmIdentifier				
signature Value					SIGNATURE ASSIGNED BY ATTRIBUTE AUTHORITY
Optional Features					

FIG. 5

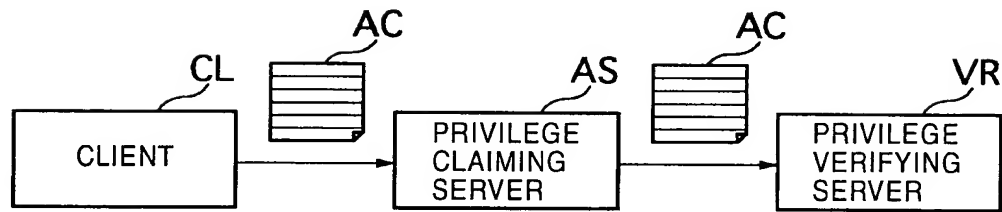


FIG. 6

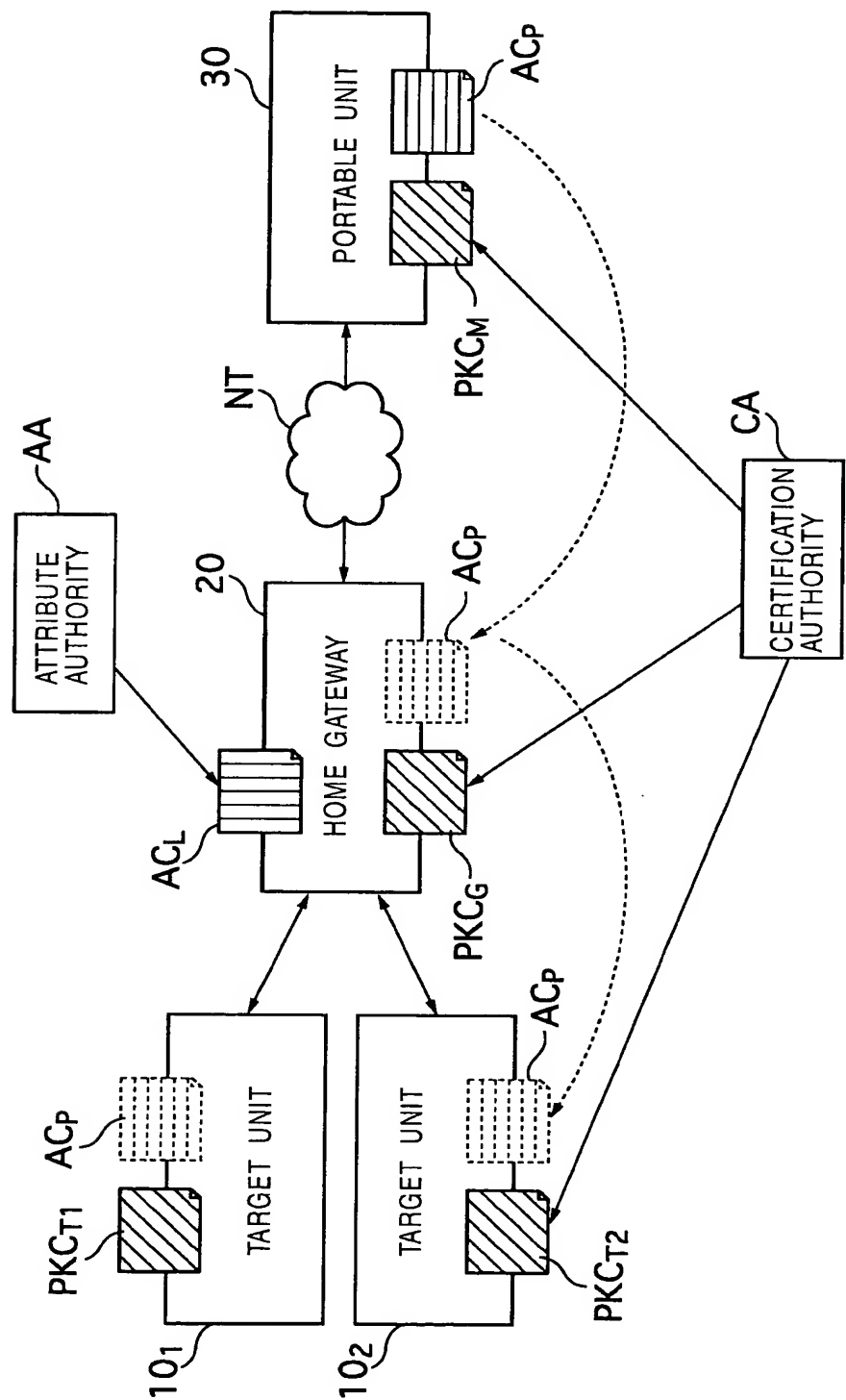


FIG. 7

ITEM	OID	VALUE
Service Authentication Information	id-aca 1	INFORMATION REQUIRED FOR SERVICE OR AUTHENTICATION
Access Identity	id-aca 2	OWNER IDENTIFIER USED WHEN OWNER ATTRIBUTE IS VERIFIED
Charging Identity	id-aca 3	ID USED FOR SERVICE ACCOUNTING
Group	id-aca 4	INFORMATION OF GROUP TO WHICH OWNER BELONGS
Role	id-at 72	NAME OF ROLE AUTHORITY, ROLE NAME

FIG. 8

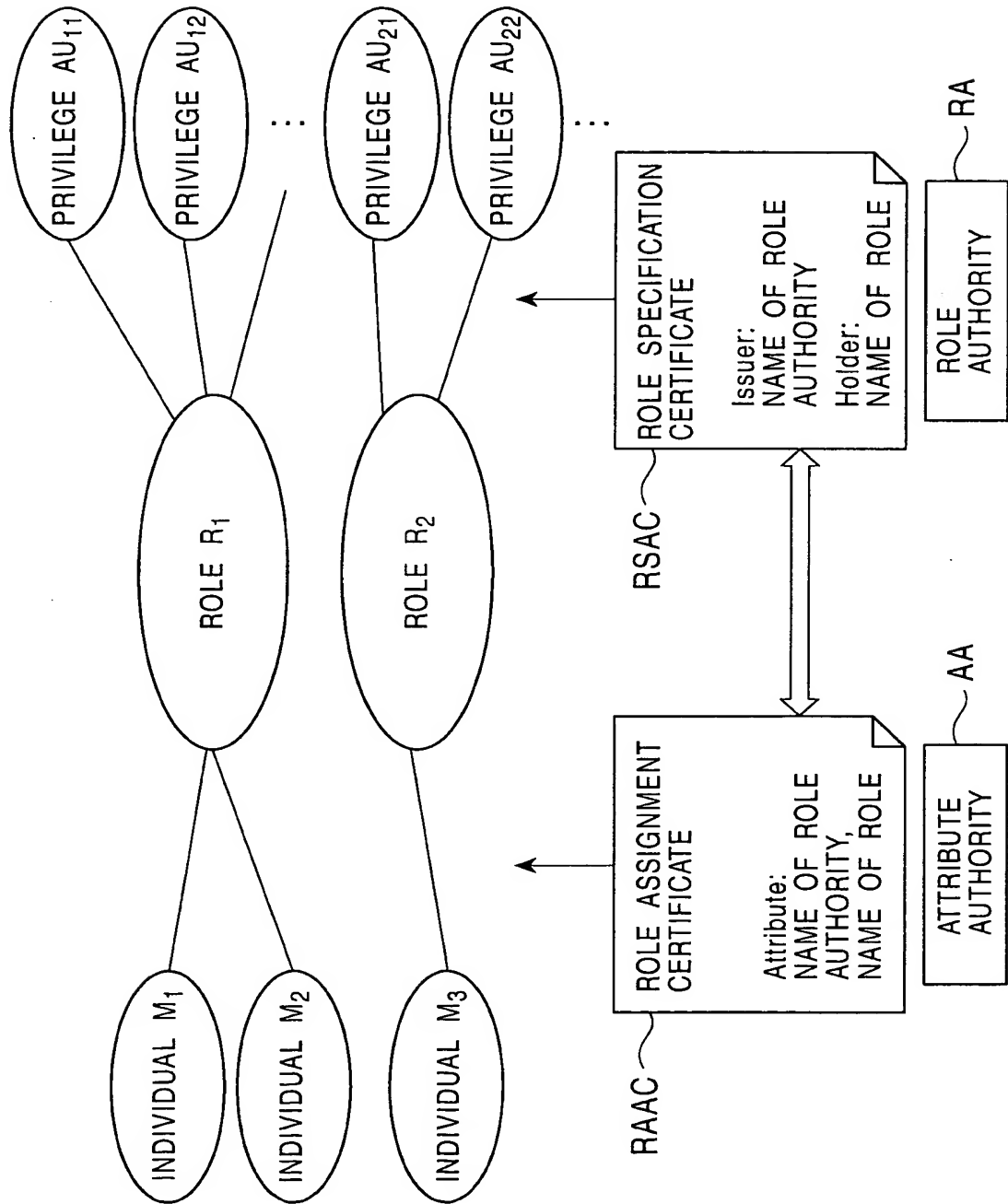


FIG. 9

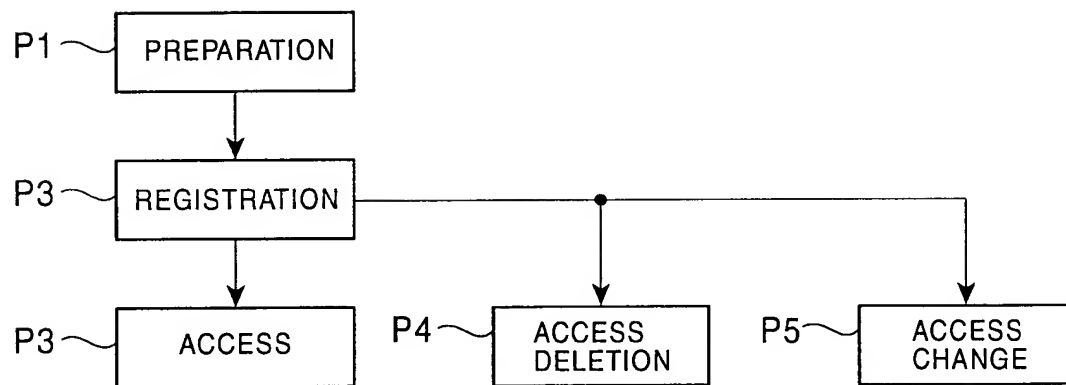
ITEM	OID	VALUE
Authority Information Access		ISSUER INFORMATION OF ATTRIBUTE CERTIFICATE, OCSP INFORMATION
Authority Key Identifier		PUBLIC-KEY INFORMATION OF ISSUER OF ATTRIBUTE CERTIFICATE
CRL Distribution Points		URI OF CRL DISTRIBUTION POINT
Audit Identity		ID OF OWNER OF ATTRIBUTE CERTIFICATE FOR INSPECTION (USED FOR TRACKING LOG. ANONYMOUS BUT CAN IDENTIFY OWNER TOGETHER WITH INFORMATION AT ATTRIBUTE AUTHORITY)
Time Specification		TIME ZONE WHEN PRIVILEGE IS EFFECTIVE
Targeting Information		SERVER NAME WITH WHICH ATTRIBUTE CERTIFICATE CAN BE RECEIVED
Proxy Info		POSSIBLE PROXY
User Notice		INFORMATION SENT TO PRIVILEGE OWNER AND PRIVILEGE INSPECTOR
PRIVILEGE POLICY		NAME OF policy authority, CHARACTER STRING OR OID VALUE
SOA (Source of Authority; ENTITY WHICH INSPECTOR TRUSTS, ROOT CA IN PKI, CORRESPONDING TO Trust anchor, TOP IN Delegation (Chain OF ATTRIBUTE AUTHORITY) (SINCE USUALLY, THERE IS ONLY ONE ATTRIBUTE AUTHORITY, ATTRIBUTE AUTHORITY IS SOA)		PRIVILEGE OF BEING ABLE TO SERVE AS SOA DESCRIPTION OF BEING SOA CERTIFICATE
PRIVILEGE TRANSFER		DESCRIBES TRANSFER CONDITION AND OTHERS REQUIRED WHEN PRIVILEGE IS TRANSFERRED TO ANOTHER ENTITY
DISCARD OF ATTRIBUTE		URI OF s DISTRIBUTION POINT
		DESCRIPTION OF NOT SUPPORTING INVALIDATION
Role		INDICATES ROLE CERTIFICATE (Role authority NAME AND ROLE NAME BY CHARACTER STRINGS)

FIG. 10

OID id-pe 10 }	VALUE
ProxyInfo :: SEQUENCE OF Targets	1.3.6.1.5.5.7.1.10
Target :: CHOICE {	
targetName[0] GeneralName,	EXAMPLE: ADDRESS OR IDENTIFIER
targetGroup[1] GeneralName,	OF HOME GATEWAY
targetCert[2] TargetCert	EXAMPLE: PUBLIC-KEY CERTIFICATE
}	OF HOME GATEWAY
TargetCert :: SEQUENCE {	
targetCertificate IssuerSerial,	
targetName GeneralName OPTIONAL,	
certDigestInfo ObjectDigestInfo OPTIONAL	
}	

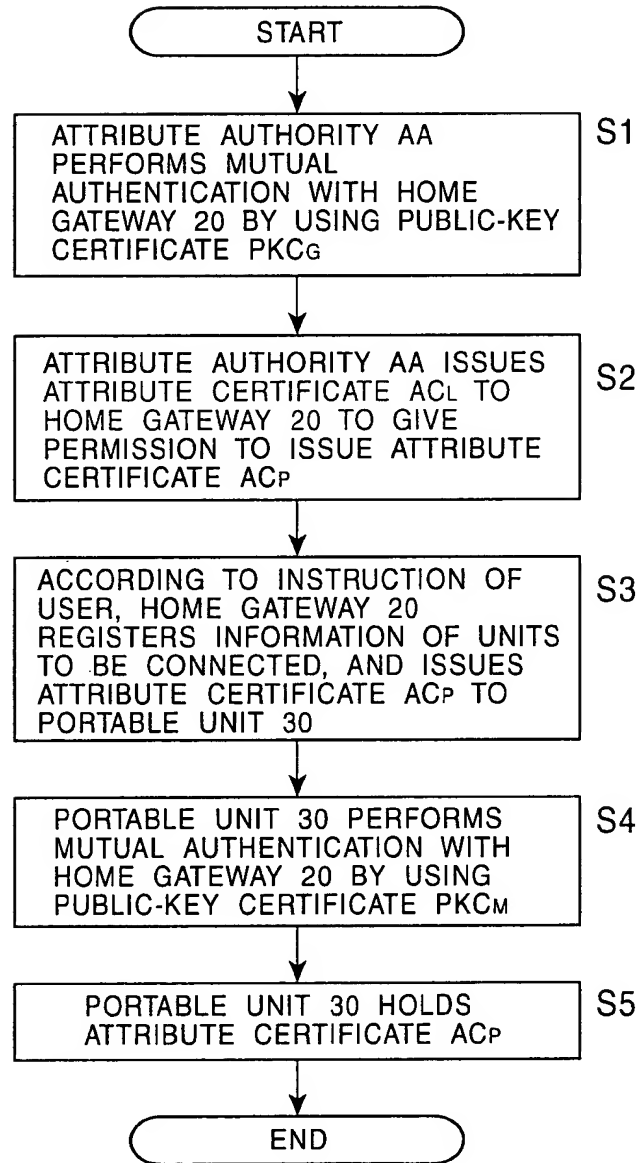
11 / 20

FIG. 11



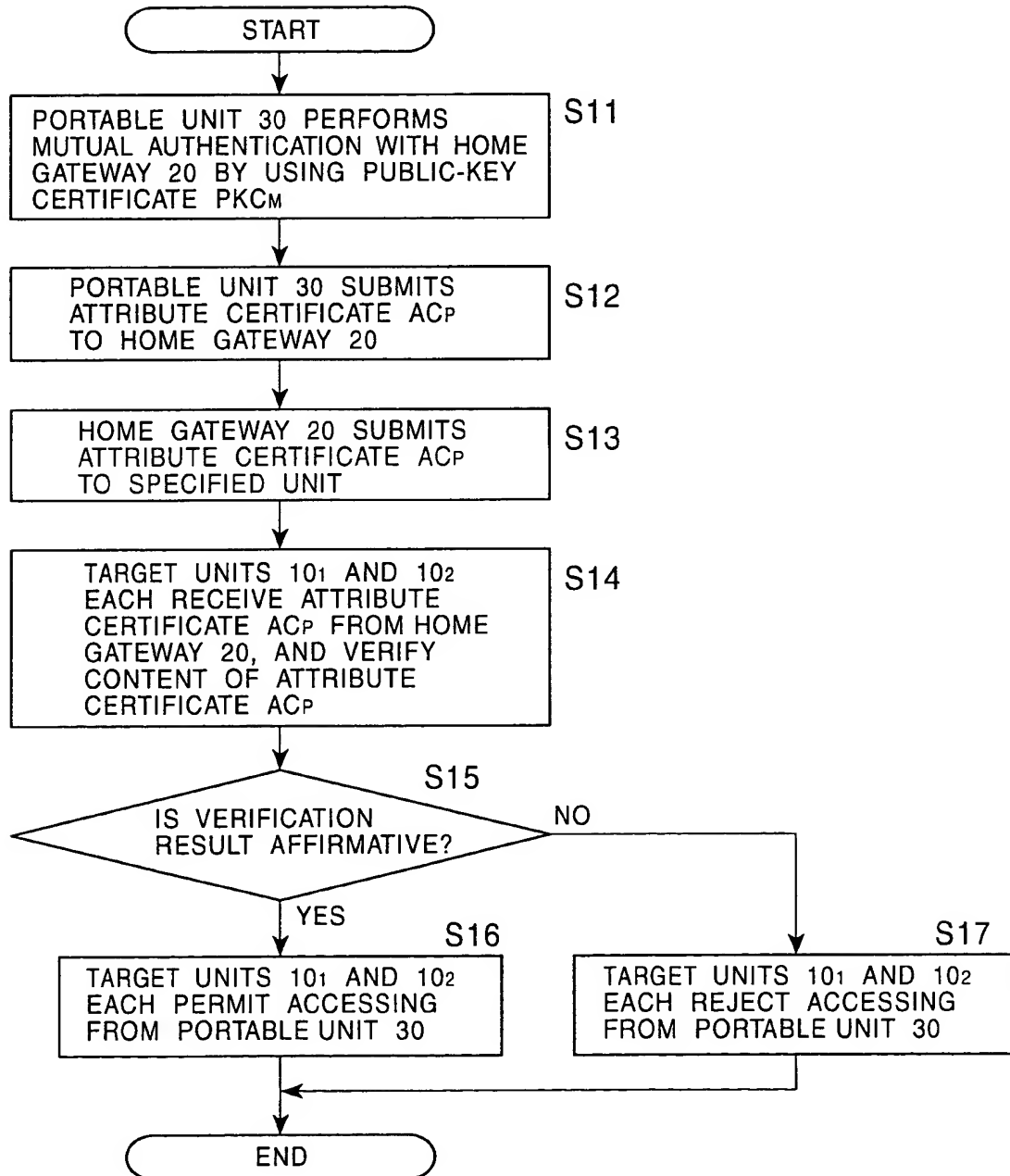
12 / 20

FIG. 12



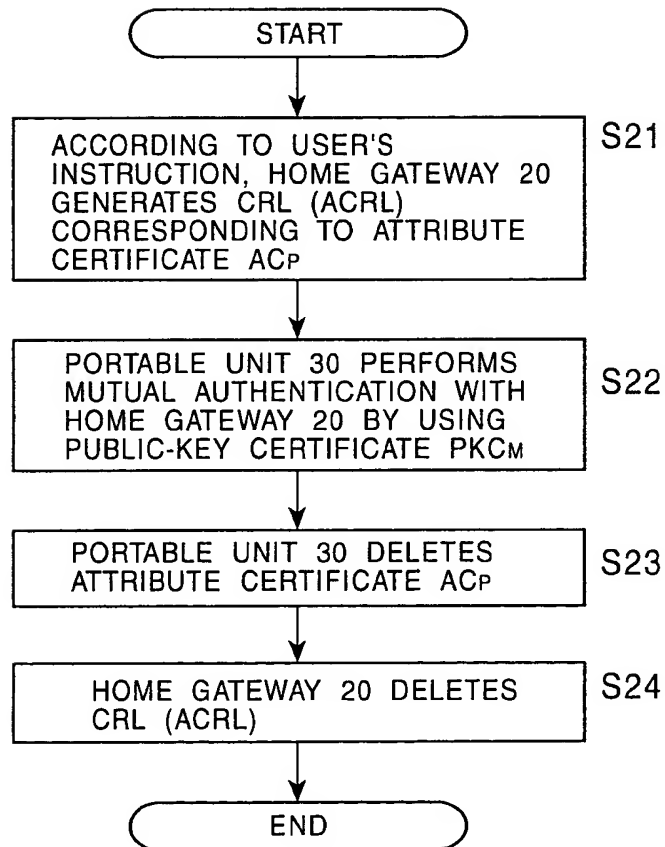
13 / 20

FIG. 13



14 / 20

FIG. 14



15 / 20

FIG. 15

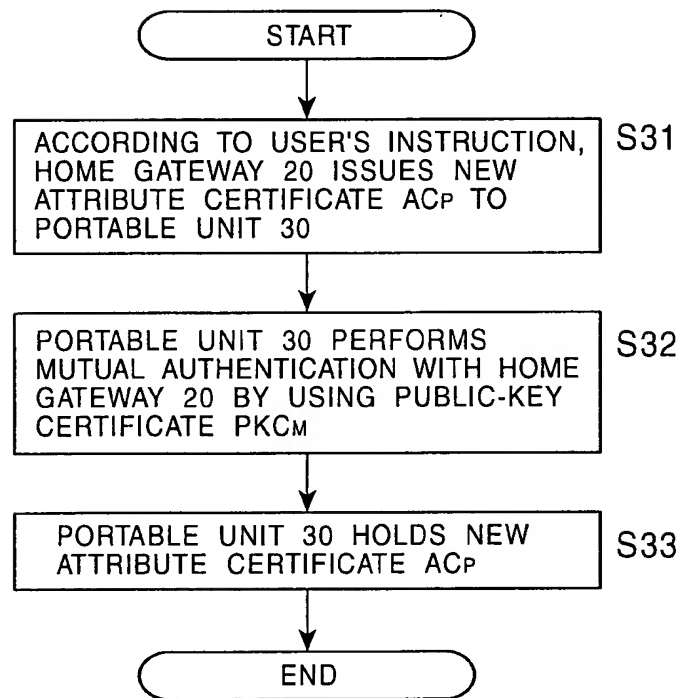
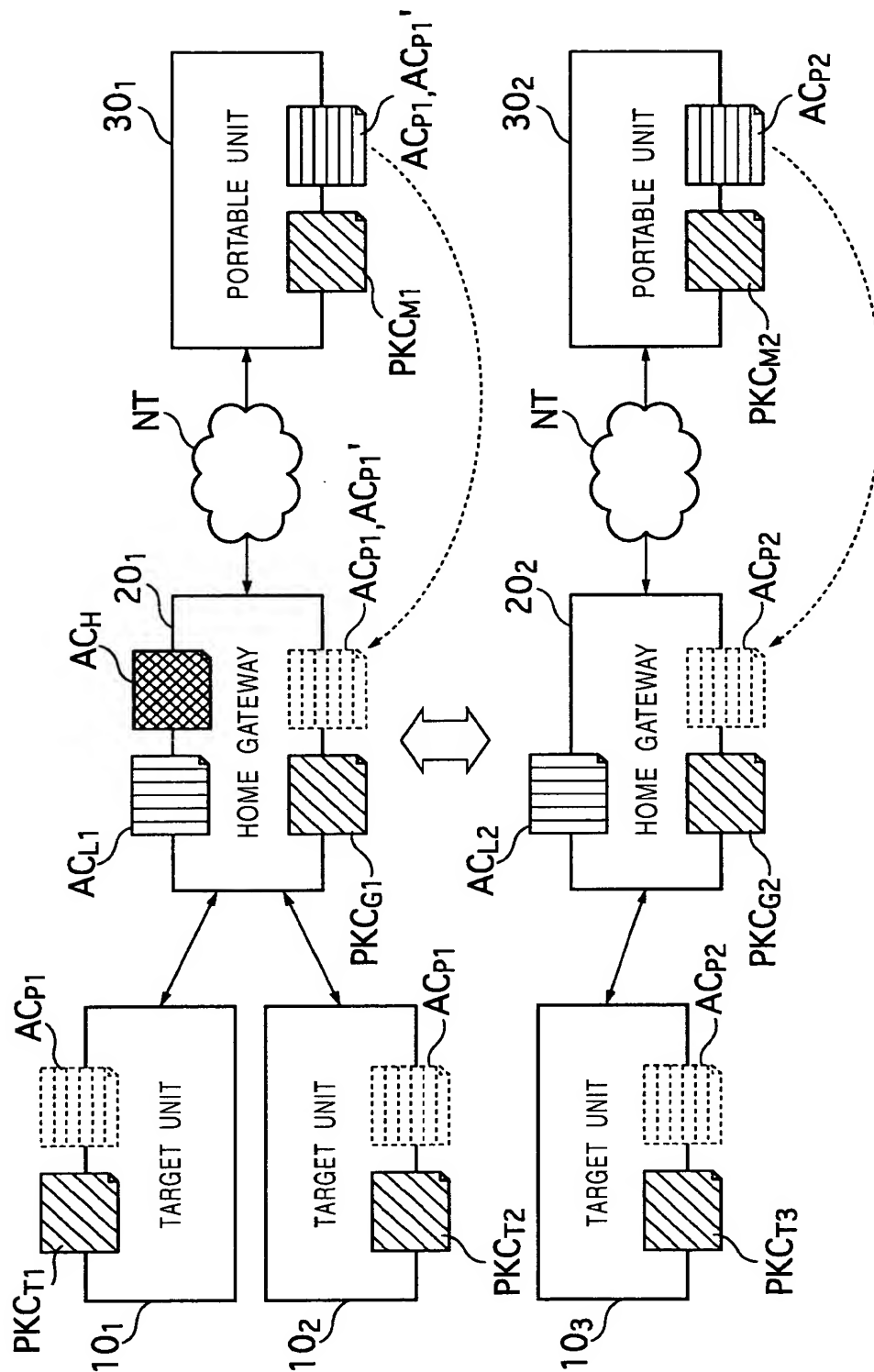
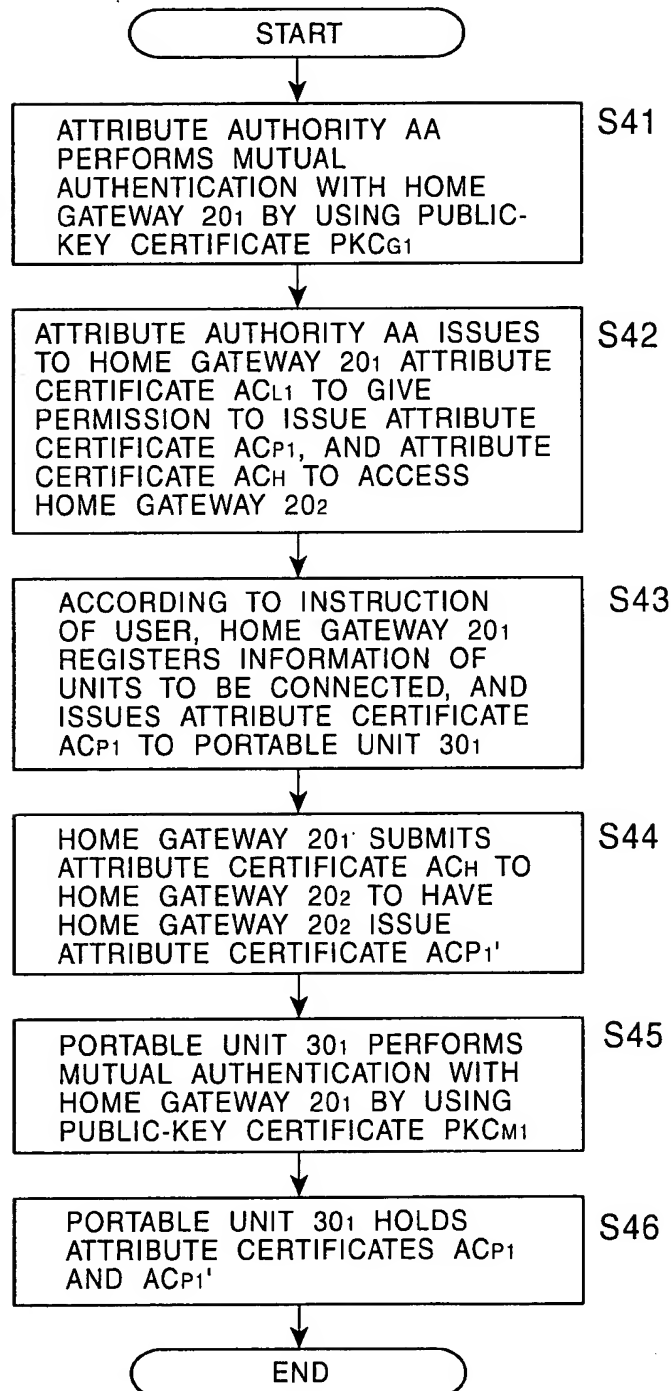


FIG. 16



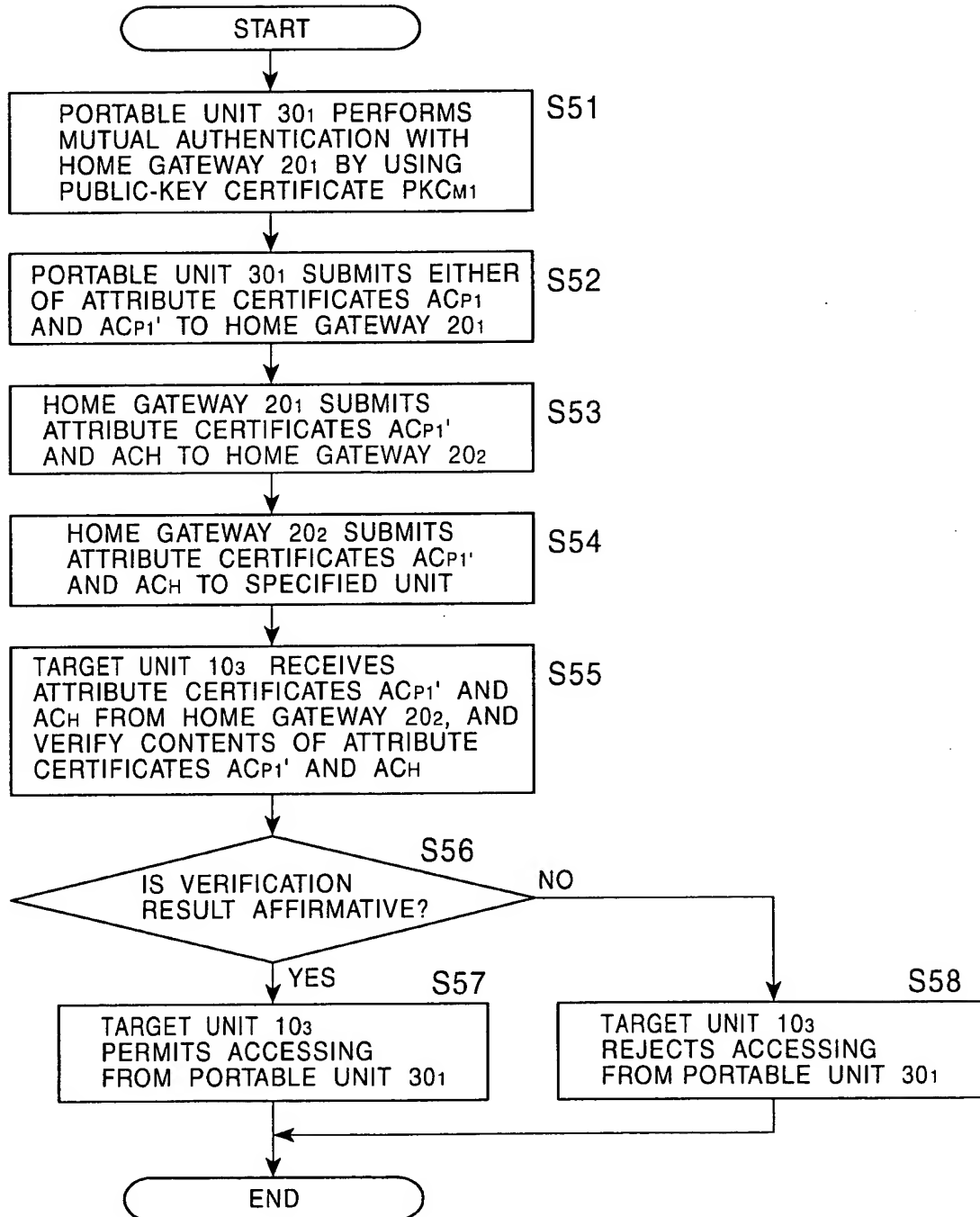
17 / 20

FIG. 17



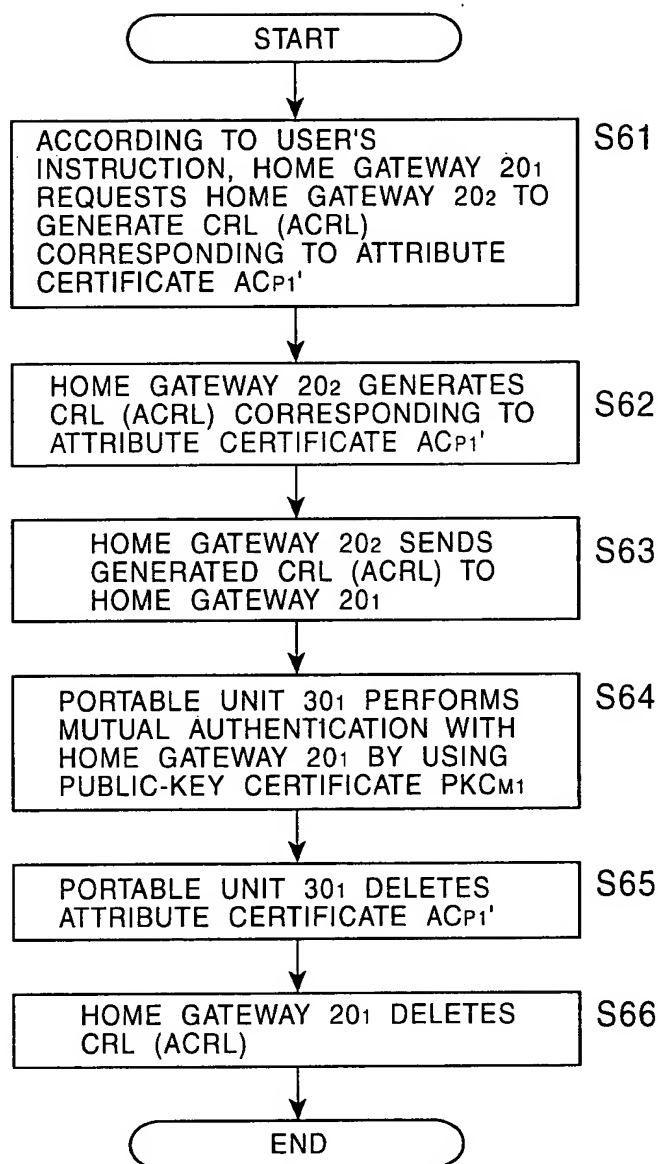
18 / 20

FIG. 18



19 / 20

FIG. 19



20 / 20

FIG. 20

